

United States District Court  
for the  
Western District of New York

In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

A black, Cyanogen cellular phone bearing FCC ID: 2ABZ2-A0001 in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8<sup>th</sup> Floor, Buffalo, NY 14202 **Case No. 18-mj-1050**

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

A black, Cyanogen cellular phone bearing FCC ID: 2ABZ2-A0001 in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8<sup>th</sup> Floor, Buffalo, NY 14202, as further described in Attachment A, attached hereto,

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*.  
See Attachment B, attached hereto and incorporated herein by reference.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
\_\_\_\_\_  
*Applicant's signature*  
NICHOLAS MELCHIORRE  
SPECIAL AGENT  
HOMELAND SECURITY INVESTIGATIONS  
\_\_\_\_\_  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: April 16, 2018

City and state: Buffalo, New York

  
\_\_\_\_\_  
*Judge's signature*  
JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE  
\_\_\_\_\_  
*Printed name and Title*

**ATTACHMENT A**

**(Schedule of Items to be Searched)**

1. **SUBJECT DEVICE - a black colored Cyanogen cellular telephone bearing FCC ID: 2ABZ2-A0001. This cellular phone was detained by law enforcement on April 4, 2018, and is in currently in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8<sup>th</sup> Floor, Buffalo, NY 14202.**

**ATTACHMENT B**

**Schedule of Items to be Searched for and Seized from the SUBJECT DEVICE**

All stored content related to the possession, receipt, and/or distribution of child pornography as defined in Title 18, United States Code, Section 2256, including, but not limited to:

Photographs, videos, web browsing history, cookies, deleted files, personal telephone and address books, text messages (incoming and outgoing), e-mail, recent calls (incoming and outgoing), missed calls, contact lists, digital codes, appointment calendars, personal notes and other items reflecting names, addresses, telephone numbers, and communications.

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT APPLICATION**

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     SS:  
CITY OF BUFFALO        )

**NICHOLAS MELCHIORRE**, being duly sworn, deposes and states:

1. I have been employed as a Special Agent (SA) with Homeland Security Investigations (HSI), within the Department of Homeland Security (DHS), since 2010. As a Special Agent, I am a federal law enforcement officer within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, federal criminal offenses.

2. I have participated in investigations targeting individuals involved in the receipt, distribution and possession of child pornography, in violation of Title 18, United States Code, Section 2252A(a)(2)(A) and Title 18, United States Code, Section 2252A(a)(5)(B). I have received specialized training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous images and videos of child pornography, as defined in Title 18, United States Code, Section 2256. As part of my employment with HSI, I successfully completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the Immigration and Customs Enforcement Basic School, both of which included instruction

with respect to the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints, and other legal processes.

3. I make this affidavit in support of an application to search the cellular telephone of RANDY COLUCCI, seized incident to his April 4, 2018 arrest, identified as a black, Cyanogen cellular phone bearing FCC ID: 2ABZ2-A0001) [hereinafter SUBJECT DEVICE]. The SUBJECT device is currently in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8<sup>th</sup> Floor, Buffalo, NY 14202.

4. As set forth in more detail below, there is probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(2)(A) (receipt and distribution of child pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) are located within the SUBJECT DEVICE.

5. The statements contained in this affidavit are based upon my investigation, information provided to me by other law enforcement personnel, and on my experience and training as a Special Agent of HSI. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A(a)(2)(A), and Section 2252A(a)(5)(B) are present on the SUBJECT DEVICE.

### **BACKGROUND OF THE INVESTIGATION**

6. On April 19, 2017, HSI SA William Aiello conducted an online investigation of the Peer to Peer (P2P) file sharing network BitTorrent for offenders sharing child pornography. Using a computer running investigative BitTorrent software, SA Aiello directly connected to the device (herein after SUSPECT DEVICE) using Internet Protocol (herein after IP) address 98.4.118.187. The SUSPECT DEVICE was targeted because it was associated with a torrent with the info hash: 952f899e8c2b81a6524f04e8fcbf259477e876de. This torrent references 139 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

7. SA Aiello was able to directly connect to the SUSPECT DEVICE and identified it as running BitTorrent client software –UT340B- uTorrent 3.4. Between 0216 and 0403 hours, SA Aiello successfully completed the download of 74 files the SUSEPCT DEVICE was making available. The SUSEPCT DEVICE was the sole candidate for each download, and as such, each file was directly downloaded from IP address 98.4.118.187. SA Ailleo reviewed several of the downloaded files which all appeared to meet the definition of child pornography as defined by Title 18, United States Code, Section 2256.

8. On April 21, 2017, SA Aiello queried IP address 98.4.118.187 through the American Registry for Internet Numbers (ARIN) which identified the IP address as registered to Time Warner Cable Internet LLC. Further open source queries identified the IP address as resolving to the Buffalo, New York area.

9. On April 21, 2017, SA Aiello sent a Department of Homeland Security administrative summons to Time Warner Cable for subscriber information for IP address 98.4.118.187 at the time of the downloads. On April 25, 2017, Time Warner Cable complied with the legal process and identified the subscriber of IP address 98.4.118.187 on April 19, 2017 as: Valerie Colucci, 1106 22<sup>nd</sup> Street, Niagara Falls, NY. The account was activated on June 5, 2014 and was still active on April 19, 2017.

#### **BACKGROUND ON PEER TO PEER FILE SHARING**

10. Peer to Peer (hereinafter P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

11. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users.

Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file.

12. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

#### **SEARCH WARRANT AND SUBSEQUENT INVESTIGATION**

13. On June 8, 2017, United States Magistrate Judge Hugh B. Scott approved a federal search warrant authorizing the search of COLUCCI's residence located at 1106 22<sup>nd</sup> Street, Niagara Falls, NY (herein after SUBJECT PREMISES), which was executed on June 19, 2017. During the execution of the search warrant, several items of evidence were located and seized, including a Gateway desktop computer serial number 0028433431, a Cricket Alcatel cellular phone model 40600, an Asus laptop computer serial number K553MA-DBOITQ, a Hewlett Packard laptop serial number 5CD2213H09, a ZTE cellular phone IMEI: 862147036031173, and a Seagate hard drive serial number 3QD0SBT7.

14. After entering and securing the SUBJECT PREMISES, COLUCCI was escorted by HSI special agents from his upstairs bedroom to the first floor of the residence.



While being escorted, COLUCCI made the unprovoked statement, "I'm fucking going back to jail. I just got out four months ago!" Once all residents were secured on the first floor, SA Aiello explained to all of the residents the purpose of the search warrant was to search of evidence of child pornography. COLUCCI interrupted and said, "That's fucking great, I'm going back to jail for this?! I changed that modem three or four times with Spectrum or Time Warner whoever they are now. We've been getting hacked."

15. SA Aiello asked COLUCCI to speak in privately outside the residence in SA Aiello's government-owned vehicle. COLUCCI agreed to give a voluntary statement to SA Aiello as witnessed by SA Michael Dombek. When SA Aiello explained the purpose of the warrant to COLUCCI, COLUCCI began the conversation by stating, "You're gonna find child pornography on there!" When COLUCCI was asked which computer the child pornography would be found on, to which he stated the laptop in his room that he showed to the agents that escorted him from his bedroom. COLUCCI stated the child pornography got on the laptop by "popping up all the time." He further explained that "all the perverts who live around me have been hacking the internet at my house." COLUCCI stated he knew he was being hacked because all of the "stuff" popping up on his computer. COLUCCI further stated that he changed out the modem at his residence at least three times because of the hacking. COLUCCI denied using P2P programs such as BitTorrent. When COLUCCI was asked specifically if he used torrent websites such as uTorrent, he confirmed he did in fact use uTorrent to download movies and music. COLUCCI stated he owned/used the laptop in his bedroom (later identified as the HP laptop computer serial number 5CD2213H09) as well as a ZTE cellular phone (later identified as the ZTE cellular

phone IMEI: 862147036031173). COLUCCI also stated his mother owned/used a laptop, and his father owned/used a smartphone.

16. Theresa Colucci (COLUCCI's mother) was interviewed by HSI SAs Nikki Tolias and Kelly Richards while COLUCCI was being interviewed by SAs Aiello and Dombek. T. Colucci identified her computer as the laptop computer seized from the living room of the SUBJECT PREMISES (later identified as the Asus laptop computer serial number K553MA-DBOITQ). T. Colucci stated that it was possible that COLUCCI also had a profile on her laptop. T. Colucci stated the wireless internet in the SUBJECT PREMISES is password protected and the only individuals with the password were: COLUCCI; Valerie Colucci; Anthony Colucci; and herself. T. Colucci further stated that COLUCCI studied computers and had multiple computers in the SUBJECT PREMISES.

17. On October 17, 2017, your affiant interviewed V. Colucci at the SUBJECT PREMISES and was witnessed by New York State Police (NYSP) Investigator (Inv.) Kevin Jordan. V. Colucci stated she, COLUCCI, T. Colucci, and A. Colucci were the only individuals with access to the wireless internet at the SUBJECT PREMISES at the time of the June 2017 search warrant execution. V. COLUCCI stated the only device she used to access the internet at the SUBJECT PREMISES was the Cricket cellular phone she had in her possession at the time of the October 17, 2017 interview. V. Colucci denied ever using her phone to search or view for child pornography. V. Colucci further denied ever having child pornography inadvertently pop up on her cellular phone. On July 14, 2017, a month after the search warrant execution, V. Colucci received a text message from Google, Inc.

with a new access code to her account that she did not request. This was the only time V. Colucci believed someone tried to hack any of her accounts or device. V. Colucci had no knowledge of COLUCCI swapping out modems from the SUBJECT PREMISES.

18. On October 17, 2017, your affiant interviewed A. Colucci at the SUBJECT PREMISES and was witnessed by NYSP Inv. Kevin Jordan. A. Colucci identified the phone seized by HSI in June 2017 as an Alcatel cellular phone (later identified as a Cricket Alcatel Model 40600 cellular phone) that was given to him by COLUCCI just prior to the execution of the search warrant after COLUCCI got a new cellular phone. A. Colucci stated the Alcatel phone did not have cellular phone service and he only used it to browse the internet using the wireless internet at the SUBJECT PREMISES. A. Colucci further stated he never used the cellular phone to search or look at child pornography.

19. On October 17, 2017, your affiant interviewed Zachary Fouts at his residence in Lewiston, New York as was witnessed by NYSP Senior Inv. Scott Folster. COLUCCI identified Fouts as V. Colucci's ex-boyfriend who also had access to the wireless internet at the SUBJECT PREMISES around the time of the June 2017 search warrant. Fouts stated he resided with the Colucci family at the SUBJECT PREMISES in the summer of 2016 until approximately December 2016 when he moved back home with his family in Lewiston. Fouts stated he never accessed the wireless internet while residing at the SUBJECT PREMISES. Fouts stated he has unlimited cellular data on his Verizon cellular phone, and strictly used cellular data to access the internet while staying at the SUBJECT PREMISES. Fouts stated he has never accessed child pornography, nor did he ever see

anyone access child pornography while at the SUBJECT PREMISES. Fouts was unaware of the June 2017 search warrant execution at the SUBJECT PREMISES.

### **FORENSIC ANALYSIS OF SEIZED EVIDENCE**

20. HSI Computer Forensic Agent (CFA) Matthew Bloom conducted forensic analysis of the evidence seized from the SUBJECT PREMISES on June 19, 2017. In total, 266 unique images and 3 unique videos containing suspected child pornography as defined under Title 18 United States Code 2256 were contained within the seized items. Specifically, all images and videos depicting suspected child pornography were found on the Hewlett Packard laptop computer, serial number 5CD2213H09 seized from COLUCCI's bedroom. Additionally, two (2) images of suspected child pornography were found on a Seagate hard drive bearing serial number 3QD0SBT7 seized from the SUBJECT PREMISES<sup>1</sup>.

21. On March 14, 2018, your affiant reviewed all 266 unique images and 3 unique videos of suspected child pornography recovered from the evidence seized from the SUBJECT PREMISES. I have described three (3) of those image files below:

- a. **MD 5 hash: 340C30A2142B69585AA2BDED3F61A85E:** An image of a pre-pubescent blonde-haired female approximately 2-4 years of age. She is wearing a pink outfit with pink buttons. Only her torso and head is visible in the image and she appears to be asleep. An adult Caucasian male, naked

---

<sup>1</sup> The total number of suspected images of child pornography is 266. Two (2) duplicate images were located on the Seagate Hard drive.

from the waist down, has his left leg next to the minor female's right cheek and his penis pressed against the minor female's lips.

- b. **MD 5 hash: DFE563D7E23CAA5A9FFCF1E15280A3A9:** An image of a pre-pubescent black-haired Asian female approximately 4-7 years of age. She is nude wearing nothing but pink stockings lying on what appears to be a bed with white bed sheets. Her underdeveloped breasts are exposed to the viewer and her legs are spread exposing her vagina to the viewer.
- c. **MD 5 hash: 0ED38E8C1A7899771208F27E65700EDA:** An image of a pre-pubescent blonde haired female approximately 4-7 years of age. She is fully nude lying on what appears to be a bed with a white comforter with her feet toward the foreground and her face to the background of the image. She is facing the viewer with her hands under her head and her feet spread. Her underdeveloped breasts and vagina are fully exposed to the viewer.

22. Further forensic analysis of the seized evidence recovered additional evidence related to the receipt and/or distribution of child pornography. Examples include:

- a. Gateway desktop computer, serial number 0028433431 – contained Universal Resource Locators (URL): “Bestsixteen.org” 52 times; “allsexyteenz.com” 42 times; and “xxxteen.tv” 2 times.
- b. Hewlett Packard laptop computer, serial number 5CD2213H09 –

- i. 266 unique images of suspected child pornography and 3 unique videos of suspected child pornography saved in the following locations:

1. \Users\Randy\Desktop\New folder\pks
2. \Users\Randy\Desktop\New folder (7)\DCIM\thumbnails
3. \Users\Randy\Desktop\New folder (7)\WallPaper
4. \Users\Randy\Desktop\New folder (9)
5. \Users\Randy\Pictures\Gifs
6. \Users\Randy\Videos\WhoreVids
7. \Lost Files\bd company
8. \Users\Randy\Documents\New folder\pks
9. \Users\Randy\AppData\Local\Microsoft\Windows\Explorer\thumb  
cache\_96.db
10. \Users\Randy\AppData\Local\Microsoft\Windows\Explorer\thumb  
cache\_256.db
11. \Users\Randy\Pictures\Gifs\Thumbs.db

- ii. 178 Google search terms including:

1. Preteen labial abuse exam pics
2. Preteen pussy
3. 10 year old pussy

- iii. Internet Explorer 10-11 main history, user “Randy” accessed 37,821 URLs, including “hdteenvids.com”
- iv. Internet Explorer 10-11 cookies, user “Randy” accessed “hdteenvids.com” on 5/12/17
- v. Seventy-nine (79) Facebook.com chats under computer user “Randy”
- vi. 244 Yahoo web mails for recipient randy.colucci@yahoo.com
- vii. Fourteen (14) user profiles on the computer, identified as:
  - 1. Administrator (2)
  - 2. Guest (2)
  - 3. HomeGroupUser\$ (2)
  - 4. Randy (2)
  - 5. Built-in (6)
- c. ZTE cellular phone, IMEI: 862147036031173 – contained only one (1) Google account in the name of “randycolucci7@gmail.com”. The device contained eight (8) webbook markings; two (2) for “P\*E\*T\*I\*T\*E-16” at “amiteen.club”.
- d. Seagate hard drive, serial number 3QD0SBT7 –
  - i. identified the sole owner and user as “Randy”

- ii. 1,012 Google search terms, including “pthc torrents,” “pthc girl pics torrent,” and “randy colucci sentencing minutes”
- iii. Programs “BitTorrent” and “UTorrent”
- iv. 1,540 P2P files, including “pthc young children from illegal Ukrainian agency new,” “pthc 10-12 y o Russian street girls new,” and “illegal rape video of underage girl, this will not be available for long.zip”
- v. Three (3) active Torrent Transfers, including “pedo pthc nude preteen private photos and vids”. File location C:\Users\Randy\Desktop\Torrent Files, 3/27/2017 5:51:06 AM
- vi. 753 Torrent file fragments, including:
  - 1. “10-12 y o girls incest pthc by ls models,” file location Users\Randy\.frostwire5\dbs\crawldb.1\crawldb.mv.db, 3/26/2017
  - 2. “14 A fucked by brother porno pre teen sex fuck amateur wife black brunette perfect tits anal Asian blonde pedo 141213111015 a years a cum Lolita mp4.zip,” file location Users\Randy\.frostwire5\dbs\crawldb.1\crawldb.mv.db, 3/26/2017



3. "5 y o 9 y o girls pthc super quality pictures," file location  
Users\Randy\.frostwire5\dbs\crawldb.1\crawldb.mv.db,  
3/26/2017

### ARREST OF RANDY COLUCCI

23. On April 2, 2018, COLUCCI was charged by way of criminal complaint with violations of Title 18, United States Code, Sections 2252A(a)(2)(A) [Receipt of Child Pornography], and 2252A(a)(5)(B) [Possession of Child Pornography]. United States Magistrate Judge Jeremiah J. McCarthy issued a federal arrest warrant for COLUCCI the same day.

24. On April 4, 2018, your Affiant and HSI SA Bryan Jacobson arrested COLUCCI pursuant to the federal arrest warrant at the New York State Parole Office in Niagara Falls, New York in the presence of New York State Parole Officer Njabulo Dlodlo.

25. Prior to transporting COLUCCI to the federal courthouse in Buffalo, New York for an initial appearance, COLUCCI consented to the release of all personal property to his girlfriend Breana Schram who was present with him at the New York State Parole Office at the time of his arrest. Your affiant released the property to Schram per COLUCCI's request.

26. During the property release process, your affiant informed COLUCCI that the cellular phone in his possession at the time of arrest (identified as a black, Cyanogen

cellular phone bearing FCC ID: 2ABZ2-A0001) [hereinafter SUBJECT DEVICE] was being detained and to turn it over to your Affiant.

27. After receiving the cellular phone from COLUCCI, your Affiant immediately noticed a black screen with scrolling script at the top of the screen consistent with a factory reset. Your affiant immediately turned the phone off and transported it to the HSI Buffalo, New York where it was secured in evidence bag A2627459 and chain of custody documented on DHS form 6051D 1442757.

28. Due to potential evidence destruction, HSI Computer Forensic Agent (CFA) James Donohue completed a digital search of the SUBJECT DEVICE, however the results of the search have not been opened by anyone in law enforcement at this time.

#### **AUTHORIZATION TO SEARCH AND SEIZE**

29. Accordingly, the application seeks authorization to search the seized identified cellular phone listed in **Attachment A**, which is attached hereto and incorporated by reference as though set forth fully herein. I believe evidence of possessing, receiving and distributing child pornography will be found within the identified SUBJECT DEVICE. The specific evidence in this regard is detailed in the Schedule of Items to be Searched for and Seized listed in **Attachment B**, which is attached hereto and incorporated by reference as though set forth fully herein.

30. While your Affiant, beyond that information set forth above, has no specific information that information pertaining to the possession of child pornography are presently being stored within the identified SUBJECT DEVICE, based on my training, my experience, my participation in this investigation, and my discussions with other experienced law enforcement personnel, I have learned:

- a. Those who attempt to, or successfully factory reset electronic devices prior to law enforcement being able to search them, do so to conceal evidence of unlawful activity.
- b. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- c. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, digital images, digital videos, websites, drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification.
- d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in

a safe, secure and private environment, such as a computer and/or cellular phone. These collections are often maintained for several years and are kept close by, usually at the individual's residence or on their person, to enable the collector to view the collection, which is valued highly.

- e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period, and often maintain child pornography within their area of control. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

### CONCLUSION

Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(2)(A) and Title 18, United States Code, Section

2252A(a)(5)(B), as specifically described in **Attachment B** to this application, are presently located within the SUBJECT DEVICE. The undersigned therefore respectfully requests that the attached warrant be issued authorizing a search for the items listed in Attachment B within the SUBJECT DEVICE, more particularly described in Attachment A to this application.



---

NICHOLAS MELCHIORRE  
Special Agent  
Homeland Security Investigations

Sworn to and subscribed before  
me this 16<sup>th</sup> day of April, 2018.



---

JEREMIAH J. MCCARTHY  
United States Magistrate Judge

**ATTACHMENT A**

**(Schedule of Items to be Searched)**

1. SUBJECT DEVICE - a black colored Cyanogen cellular telephone bearing FCC ID: 2ABZ2-A0001. This cellular phone was detained by law enforcement on April 4, 2018, and is in currently in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8<sup>th</sup> Floor, Buffalo, NY 14202.

**ATTACHMENT B**

**Schedule of Items to be Searched for and Seized from the SUBJECT DEVICE**

All stored content related to the possession, receipt, and/or distribution of child pornography as defined in Title 18, United States Code, Section 2256, including, but not limited to:

Photographs, videos, web browsing history, cookies, deleted files, personal telephone and address books, text messages (incoming and outgoing), e-mail, recent calls (incoming and outgoing), missed calls, contact lists, digital codes, appointment calendars, personal notes and other items reflecting names, addresses, telephone numbers, and communications.